



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/710,426	07/09/2004	Chenming Chuang	22171-00018-US1	4425
30678 7590 09/14/2007 CONNOLLY BOVE LODGE & HUTZ LLP 1875 EYE STREET, N.W. SUITE 1100 WASHINGTON, DC 20036			EXAMINER AVERY, JEREMIAH L	
			ART UNIT 2131	PAPER NUMBER
			MAIL DATE 09/14/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/710,426

Applicant(s)

CHUANG, CHENMING

Examiner

Jeremiah Avery

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 02 July 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09 July 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application
- ☐ Other: _____

DETAILED ACTION

1. Claims 1-14 have been examined.
2. Responses to Applicant's remarks have been given.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-14 are rejected under 35 U.S.C. 102(b) as being anticipated by United States Patent No. 6,233,565 to Lewis et al., hereinafter Lewis.

1. Regarding claim 1, Lewis teaches a method of secure data exchange between a master cryptographic unit and a slave cryptographic unit, comprising the steps of:
sending either a reset message or a key validation message to request the master cryptographic unit to validate a key held by the slave cryptographic unit during each session (column 15, lines 47-64, "entries are checked against the customer record in the Master Database 305", column 19, lines 60-67, column 20, lines 1-15 and 57-67, column 21, lines 64-67; column 22, lines 1-9, 16-25 and 42-67, column 23, lines 1-22 and 35-48, "session keys exchanged", column 24, lines 16-37 and 54-67, column 25, lines 1-28, "at which point the counter will reset to 1" and "Transaction Manager will complete the transaction by sending a receipt, including a digital signature as evidence of payment for the transaction" and lines 53-67, column 26, lines 1-12, column 28, lines 14-28 and 50-67, column 29, lines 1-35 and 49-67, column 30, lines 1-9, 14-29, column 31, lines 5-15 and column 32, lines 34-39);
forwarding a key exchange message, which includes a new key encrypted through the key held by the slave cryptographic unit, from the master cryptographic unit to the slave

Art Unit: 2131

cryptographic unit (column 15, lines 47-64, "the customer 2n will receive a public key and a private key pair file in encrypted form from the web server 150", column 19, lines 60-67, column 20, lines 1-15 and 57-67, column 21, lines 64-67, column 22, lines 1-9, 16-25 and 42-67, column 23, lines 1-22 and 35-48, "session keys exchanged", column 24, lines 16-37 and 54-67, column 25, lines 1-28 and 53-67, column 26, lines 1-12, column 28, lines 14-28 and 50-67, column 29, lines 1-35 and 49-67, column 30, lines 1-9, 14-29, column 31, lines 5-15 and column 32, lines 34-39).

2. Regarding claim 2, Lewis teaches a step of sending a key confirmation message to notify the master cryptographic unit that the new key is correctly received by the slave cryptographic unit (column 25, lines 1-28 and 61-67, column 26, lines 1-12, column 28, lines 20-28 and 50-67, column 29, lines 1-40, "recipient uses the hash to ensure message integrity" and lines 49-67, "mailed to the client", column 30, lines 1-29 and column 32, lines 34-39).

3. Regarding claim 3, Lewis teaches responding to the key confirmation message with a downloading message to allow the slave cryptographic unit to retrieve requested information (column 11, lines 46-57, "customer then downloads the client software program for operating the system", column 15, lines 47-67, "If the customer number and password are valid, the download will proceed", column 16, lines 1-4 and column 22, lines 50-57);

sending a finish message to the master cryptographic unit after the requested information is completely downloaded (column 16, lines 18-43, column 17, lines 4-15, "A

Art Unit: 2131

'result' code is passed back to the purchase server 190 to indicate whether the credit card has been approved or not" and column 29, lines 20-26, "the protocol is complete").

4. Regarding claim 4, Lewis teaches wherein the reset message requests the master cryptographic unit to validate an initial key held by the slave cryptographic unit (column 4, lines 18-35, column 6, lines 1-15, column 15, lines 47-64, column 18, lines 2-8, "confirming the success or failure of the transaction", column 19, lines 60-67, column 20, lines 61-67, column 22, lines 42-67, "Key File will contain the necessary information to uniquely identify and authenticate a client 2n to the server 4", column 24, lines 16-33, column 28, lines 50-61, column 29, lines 20-35 and column 32, lines 34-39).

5. Regarding claim 5, Lewis teaches wherein the initial key is either pre-configured by factories and permanently stored in the slave cryptographic unit or obtained from the master cryptographic unit through a manual login (column 11, lines 46-66, column 15, lines 47-64, "the customer 2n will receive a public key and a private key pair file in encrypted form from the web server 150", column 22, lines 2-9 and 42-67, column 23, lines 1-8, column 24, lines 16-33, column 28, lines 21-28 and 50-67, column 29, lines 1-11 and 49-62, "server 4 initially produces the client authentication keys" and column 30, lines 13-29).

6. Regarding claim 6, Lewis teaches a step of notifying the slave cryptographic unit that the key is invalid after the key validation message is sent (column 20, lines 61-67, "Invalid information will be identified once valid information is provided", column 29, lines 62-67 and column 30, lines 1-11, "After a client 2n authenticates with the server 4, the server 4 will notify the client if the keys have expired").

7. Regarding claim 7, Lewis teaches a step of sending the reset message to request the master cryptographic unit to validate an initial key held by the slave cryptographic unit (column 4, lines 18-35, column 6, lines 1-15, column 15, lines 47-64, column 18, lines 2-8, "confirming the success or failure of the transaction", column 19, lines 60-67, column 20, lines 61-67, column 22, lines 42-67, "Key File will contain the necessary information to uniquely identify and authenticate a client 2n to the server 4", column 24, lines 16-33, column 25, lines 1-15, "at which point the counter will reset to 1", column 28, lines 50-61, column 29, lines 20-35 and column 32, lines 34-39).

8. Regarding claim 8, Lewis teaches sending another key validation message to request the master cryptographic unit to validate the new key held by the slave cryptographic unit (column 4, lines 18-35, column 6, lines 1-15, column 15, lines 47-64, column 18, lines 2-8, "confirming the success or failure of the transaction", column 19, lines 60-67, column 20, lines 61-67, column 22, lines 42-67, "Key File will contain the necessary information to uniquely identify and authenticate a client 2n to the server 4", column 23, lines 10-22, "re-generate a new pair of public and private keys 532", column 24, lines 16-33, column 28, lines 50-61, column 29, lines 20-35 and column 32, lines 34-39);

forwarding another key exchange message, which includes a renewed key encrypted through the new key held by the slave cryptographic unit (column 4, lines 18-35, column 6, lines 1-15, column 15, lines 47-64, column 18, lines 2-8, "confirming the success or failure of the transaction", column 19, lines 60-67, column 20, lines 61-67, column 22, lines 42-67, "Key File will contain the necessary information to uniquely identify and

Art Unit: 2131

authenticate a client 2n to the server 4", column 23, lines 10-22, "re-generate a new pair of public and private keys 532" and lines 36-48, column 24, lines 16-33, column 28, lines 50-61, column 29, lines 20-35 and column 32, lines 34-39).

9. Regarding claim 9, Lewis teaches a step of notifying the slave cryptographic unit that the key is invalid after the reset message is sent (column 20, lines 61-67, "Invalid information will be identified once valid information is provided", column 29, lines 62-67 and column 30, lines 1-11, "After a client 2n authenticates with the server 4, the server 4 will notify the client if the keys have expired").

10. Regarding claim 10, Lewis teaches wherein the master cryptographic unit is a key distribution server (column 15, lines 47-64, "the customer 2n will receive a public key and a private key pair file in encrypted form from the web server 150", column 19, lines 60-67, column 20, lines 1-15 and 57-67, column 21, lines 64-67, column 22, lines 1-9, 16-25 and 42-67, column 23, lines 1-22 and 35-48, "session keys exchanged", column 24, lines 16-37 and 54-67, column 25, lines 1-28 and 53-67, column 26, lines 1-12, column 28, lines 14-28 and 50-67, column 29, lines 1-35 and 49-67, column 30, lines 1-9, 14-29, column 31, lines 5-15 and column 32, lines 34-39).

11. Regarding claim 11, Lewis teaches wherein the key distribution server is included in an automatic provisioning system (column 15, lines 47-64, "If the customer number and password are valid, the download will proceed", column 23, lines 35-48, column 24, lines 16-33 and column 35, lines 51-62).

12. Regarding claim 12, Lewis wherein the slave cryptographic unit is a client (column 15, lines 47-64, "the customer 2n will receive a public key and a private key

Art Unit: 2131

pair file in encrypted form from the web server 150", column 19, lines 60-67, column 20, lines 1-15 and 57-67, column 21, lines 64-67, column 22, lines 1-9, 16-25 and 42-67, "Key File will contain the necessary information to uniquely identify and authenticate a client 2n to the server 4", column 23, lines 1-22 and 35-48, "session keys exchanged", column 24, lines 16-37 and 54-67, column 25, lines 1-28 and 53-67, column 26, lines 1-12, column 28, lines 14-28 and 50-67, column 29, lines 1-35 and 49-67, column 30, lines 1-9, 14-29, column 31, lines 5-15 and column 32, lines 34-39).

13. Regarding claim 13, Lewis teaches wherein the reset message includes an initial key, a physical address of the slave cryptographic unit, timestamp data and hash data (column 5, lines 11-26 and 54-58, column 6, lines 1-15, column 15, lines 47-64, column 19, lines 52-67, column 21, lines 39-67, "proof of valid physical address will be initially established", column 22, lines 42-67, "Key File will contain the necessary information to uniquely identify and authenticate a client 2n to the server 4", column 23, lines 1-22, column 25, lines 1-15, "date/time stamp", column 27, lines 25-39, "a new user 2n would contact the server 4 with information that uniquely identifies him/herself", column 29, lines 1-11 and 49-67 and column 30, lines 1-11).

14. Regarding claim 14, Lewis teaches wherein the key validation message includes the key, a physical address of the slave cryptographic unit, timestamp data and hash data (column 5, lines 11-26 and 54-58, column 6, lines 1-15, column 15, lines 47-64, column 19, lines 52-67, column 21, lines 39-67, "proof of valid physical address will be initially established", column 22, lines 42-67, "Key File will contain the necessary information to uniquely identify and authenticate a client 2n to the server 4", column 23,

lines 1-22, column 25, lines 1-15, "date/time stamp", column 27, lines 25-39, "a new user 2n would contact the server 4 with information that uniquely identifies him/herself", column 29, lines 1-11 and 49-67 and column 30, lines 1-11).

15. With regards to claims 13 and 14, it is known in the art that within a client/server environment, the location or "address" of each respective device will exist and be known between said client and server.

Response to Arguments

16. Applicant's arguments, see pages 5 and 6, filed 07/02/07, with respect to the objections of claims 3 and 7 have been fully considered and are persuasive. The objections of claims 3 and 7 have been withdrawn.

17. Applicant's arguments, see page 6, filed 07/02/07, with respect to the 35 U.S.C. 112, 2nd paragraph rejection of claims 7 and 9 have been fully considered and are persuasive. The 35 U.S.C. 112, 2nd paragraph rejection of claims 7 and 9 have been withdrawn.

18. Applicant's arguments filed 07/02/07 have been fully considered but they are not persuasive. With regards to the Applicant's arguments pertaining to the limitation of claim 1, "sending *either* a reset message *or* a key validation message to request the master cryptographic unit to validate a key held by the slave cryptographic unit during each session", the Examiner respectfully maintains the above-cited grounds of rejection; in particular but not limited to column 15, lines 47-64, "entries are checked against the customer record in the Master Database 305" and "the customer 2n will receive a public key and a private key pair file in encrypted form from the web server 150", column 18,

Art Unit: 2131

lines 2-8, "confirming the success or failure of the transaction" and column 22, lines 42-67, "Key File will contain the necessary information to uniquely identify and authenticate a client 2n to the server 4".

19. Further, with regards to the Applicant's argument that, "the present invention is based on the exchange of cryptographic keys between two cryptographic units and a new key replaces a previous key during each session", the Examiner maintains the above-cited grounds of rejection, in particular but not limited to column 23, lines 10-22, "re-generate a new pair of public and private keys 532. The client will generate a new key...".

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following United States Patents are cited to further show the state of the art with respect to secure exchange of data within a network environment, such as:

United States Patent No. 6,757,710 to Reed which is cited to show an automated communications system that operates to transfer data, metadata and methods from a provider computer to a consumer computer through a communications network.

United States Patent No. 6,704,873 to Underwood which is cited to show a secure gateway interconnection in an e-commerce based environment.

21. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2131

22. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

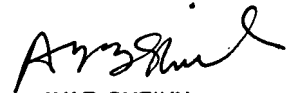
23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeremiah Avery whose telephone number is (571) 272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

24. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

25. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JLA



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100